

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization  
International Bureau



(43) International Publication Date  
7 March 2002 (07.03.2002)

PCT

(10) International Publication Number  
WO 02/19092 A1

(51) International Patent Classification<sup>7</sup>: G06F 7/04

(21) International Application Number: PCT/US01/26840

(22) International Filing Date: 28 August 2001 (28.08.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:  
60/228,555 28 August 2000 (28.08.2000) US

(71) Applicant (for all designated States except US):  
EBOX.COM INC. [CA/CA]; 4211 Yonge St., Toronto,  
Ontario M2P 2A9 (CA).

(72) Inventor; and

(75) Inventor/Applicant (for US only): STEVENS, John, K.  
[US/CA]; eBox.com, Inc., 4211 Yonge St., Toronto, On-  
tario M2P 2A9 (CA).

(74) Agent: OPPEDAH, Carl; Oppedahl & Larson LLP, P.O.  
Box 5068, Dillon, CO 80435-5068 (US).

(81) Designated States (national): AE, AG, AL, AM, AT, AU,  
AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU,  
CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH,  
GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC,  
LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW,  
MX, MZ, NO, NZ, PH, PL, PT, RO, RU, SD, SE, SG, SI,  
SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU,  
ZA, ZW.

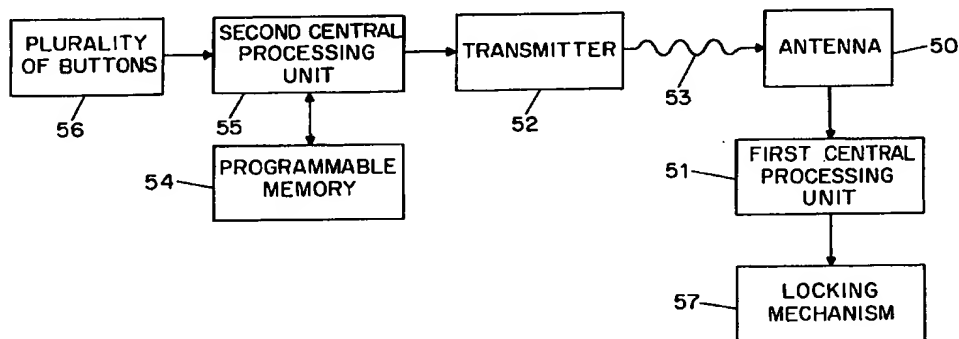
(84) Designated States (regional): ARIPO patent (GH, GM,  
KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian  
patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European  
patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE,  
IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF,  
CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD,  
TG).

Published:

- with international search report
- before the expiration of the time limit for amending the  
claims and to be republished in the event of receipt of  
amendments

For two-letter codes and other abbreviations, refer to the "Guid-  
ance Notes on Codes and Abbreviations" appearing at the begin-  
ning of each regular issue of the PCT Gazette.

(54) Title: A HIGH SECURITY WIRELESS KEY FOR ASYNCHRONOUS DELIVERY DROP BOXES



(57) Abstract: A wireless key (6), capable of transmitting an ultra-low frequency radio wave signal (5), is used to gain access to a secure receptacle (1), the wireless key (6) and receptacle (1) comprising a system to ensure the secure transfer or delivery of items between parties typically engaging in e-commerce. The wireless key (6) possesses a means to discriminate against the unauthorized entry of the receptacle, such as through the use of buttons to enter a secure access code. The wireless key (6) accepts an access code entry from the user desiring entry to the receptacle (1) and subsequently transmits an ultra-low frequency signal (5) to a receiving and processing means (4). If the analysis of the signal indicates the user of the wireless key (6) is authorized to gain entry to the receptacle (1), the receptacle's locking mechanism (3) is disengaged to allow entry.

## **A HIGH SECURITY WIRELESS KEY FOR ASYNCHRONOUS DELIVERY DROP BOXES**

### Cross Reference to Related Applications

This application claims priority from and incorporates by reference U.S. Provisional Patent Application No. 60/228,555, filed on August 28, 2001.

### 5 Background of the Invention

The present invention relates to the secure transfer of retail goods between a delivery carrier and a consumer. With the advent of e-commerce, a consumer can order a retail good through the Internet or other telecommunications means and the delivery carrier must make a delivery to the consumer and at a time that is potentially  
10 inconvenient for the consumer to receive the order. To deliver the retail goods to the consumer, the parties will make use of a secure drop box or receptacle that possesses a lock to prevent unauthorized parties, such as thieves, from accessing the drop box.

Currently, many secure receptacles employ a keypad which is physically integrated with the secure receptacle. When a delivery carrier or consumer desires to  
15 gain access to the secure receptacle, an access code is entered using the keypad. Keypads thus provide some level of security, but the access code may be compromised through either the direct observation of an authorized party entering the code, or by determining which keys have been previously depressed by inspecting the keys of the keypad.

20 Therefore, there is a need to increase the means by which security of drop boxes can be increased to ensure the delivery of retail goods to a consumer.

### Summary of the Invention

The present invention is directed towards a system for the delivery of retail  
25 goods to a secure receptacle. A wireless key transmitting an access code allows entry to the secure receptacle upon the successful processing of the access code and the subsequent disengagement of the secure receptacle's locking mechanism.

### Description of the Drawings

30 FIG. 1 shows the wireless key transmitting an unlocking signal to the antenna

cooperatively positioned within the secure receptacle.

FIG. 2 shows one embodiment of the wireless key.

FIG. 3 shows a cellular telephone acting as a wireless key through a geographically distanced central server.

5 FIG. 4 shows a two-way pager acting as a wireless key through a geographically distanced central server.

FIG. 5 shows a home computer acting as a wireless key through a geographically distanced central server.

10 FIG. 6 shows a wireless key in which the programmable memory and central processing unit of the wireless key determine whether the access code is authorized before a signal is transmitted to the antenna that is physically integrated with a secure receptacle.

FIG. 7 shows a wireless key in which unlocking signals are sent to the secure receptacle and the central processing unit and programmable memory integrated with the secure receptacle determine whether the access code entered into the wireless key is  
15 authorized.

FIG. 8 shows the process associated with the use of a wireless key, one access code, and a secure receptacle in the secure delivery of retail goods.

FIG. 9 shows the process associated with the use of a wireless key, a keypad, two access codes, and a secure receptacle in the secure delivery of retail goods.

20 FIG. 10 shows the process associated in the use of an icon that informs a consumer about how much space is left in that consumer's secure receptacle as an order for retail goods is placed.

#### Detailed Description of the Invention

25 The present invention is directed to a system that uses a wireless key and a secure receptacle in the transfer of retail goods between a consumer and a delivery carrier. The system, through the use of the wireless key, possesses several means to discriminate against those parties who are not authorized to use the wireless key for gaining access to the secure receptacle.

30 A retail good in the present invention comprises any good or service that a consumer can purchase remotely from a supplier, such as through the Internet or over

the telephone, and involves the delivery or pickup of a tangible item. Such retail goods, for example, include perishable and packaged dry goods, pharmaceutical prescriptions, and beverages. In addition, retail goods include items associated with convenience services. For example, movie rentals and the dry cleaning of clothing are retail goods as envisioned in this invention, although such "products" are closely related to the performance of a service. The present invention contemplates a retail good as anything which can be delivered and picked up at a consumer's residence by a delivery carrier and stored in a secure receptacle. Thus, the present invention contemplates the transfer of retail goods, which includes not only the delivery of items, but also the pickup of items.

The secure receptacle is designed to safely guard retail goods between the times that the retail goods are transferred between the user of the secure receptacle, the consumer, and the delivery carrier for the supplier. In order for a delivery carrier to access the secure receptacle to either pickup or deliver a retail good, the secure receptacle must be located in a place that is accessible to the rest of the public. Thus, to protect against thieves and other unauthorized persons, two variables must be addressed in securing the receptacle: securing the interior so that the contents of the receptacle remain safe, and securing the receptacle itself so as to minimize the risk of the theft of the receptacle itself.

Securing the receptacle itself may be accomplished by many means, such as attaching the receptacle to the exterior side of a house or bolting the bottom of the interior to the ground. However, the preferred embodiment of the invention is to secure the bottom of the secure receptacle (1) to a separate platform base (2), as shown in FIG. 1, that has a large weight, such as 120 pounds. A platform base of this mass allows the receptacle to be moved relatively easy, yet provides a deterrent to theft.

The receptacle possesses a locking mechanism (3), as shown in FIG.1, coupled with a central processing unit to prevent unauthorized access to the contents of the receptacle. The locking mechanism is disengaged by the central processing unit (4) only if an unlocking signal (5) is transmitted from the wireless key (6) and ultimately received by the antenna (7) and processed as acceptable by the central processing unit (4). The unlocking signal in the preferred embodiment comprises an ultra-low

frequency radio wave.

Those skilled in the art will recognize that many different electronic embodiments are possible to produce a device that comprises a wireless key. One embodiment of the invention, as shown in FIG. 2, contemplates a wireless key (6) that possesses ten buttons (8) and is conveniently shaped to be about the size of a credit card. The wireless key furthermore possesses a central processing unit that controls the transmission of the unlocking signal, and a programmable memory for storing the access code known by a party authorized to use the wireless key. Upon the entry of an access code, the central processing unit compares the entry to that stored in the first programmable memory. If the entered access code correctly matches the access code stored in the memory, an unlocking signal will be transmitted by the wireless key when the user of the wireless key presses an "OPEN" button (9).

The following examples further illustrate, without limitation, how a wireless key can be used with a secure receptacle.

#### Example 1

In one embodiment of a system for the secure delivery of a retail good, as shown in FIG. 3, a wireless key comprising a cellular telephone (20) and possessing a plurality of buttons to enter an access code transmits a first unlocking signal (21) to a geographically distant central server (22), the wireless key being physically separate from a secure receptacle and typically stored in locations inaccessible to unauthorized users of the secure receptacle. A receiving unit (23), comprising a central processing unit communicatively connected to a programmable memory, is cooperatively positioned within the secure receptacle and communicatively connected to the geographically distant central server (22). The receiving unit receives a second unlocking signal (24) from the geographically distant central server. The central processing unit of the receiving unit (23) processes the second unlocking signal (24), whereupon a locking mechanism (25) for the secure receptacle is disengaged thereby allowing entry to the secure receptacle.

#### Example 2

In one embodiment of a system for the secure delivery of a retail good, as shown in

FIG. 4, a wireless key comprising a two-way pager (30) and possessing a plurality of buttons to enter an access code transmits a first unlocking signal (31) to a geographically distant central server (32), the wireless key being physically separate from a secure receptacle and typically stored in locations inaccessible to unauthorized users of the secure receptacle. A receiving unit (33), comprising a central processing unit communicatively connected to a programmable memory, is cooperatively positioned within the secure receptacle and communicatively connected to the geographically distant central server (32). The receiving unit receives a second unlocking signal (34) from the geographically distant central server. The central processing unit of the receiving unit (33) processes the second unlocking signal (34), whereupon a locking mechanism (35) for the secure receptacle is disengaged thereby allowing entry to the secure receptacle.

#### Example 3

In one embodiment of a system for the secure delivery of a retail good, as shown in FIG. 5, a wireless key comprising a home computer with a modem (40) transmits a first unlocking signal (41) to a geographically distant central server (42), the wireless key being physically separate from a secure receptacle and typically stored in locations inaccessible to unauthorized users of the secure receptacle. A receiving unit (43), comprising a central processing unit communicatively connected to a programmable memory, is cooperatively positioned within the secure receptacle and communicatively connected to the geographically distant central server (42). The receiving unit receives a second unlocking signal (44) from the geographically distant central server. The central processing unit of the receiving unit (43) processes the second unlocking signal (44), whereupon a locking mechanism (45) for the secure receptacle is disengaged thereby allowing entry to the secure receptacle.

#### Example 4

In a further embodiment of the invention, as shown in FIG. 6, a receiving unit comprises an antenna (50) and a first central processing unit (51). The receiving unit is cooperatively positioned within a secure receptacle, the first central processing unit (51) communicatively connected to the antenna (50), and the antenna communicatively connected to a transmitter of a wireless key (52) via a wireless link (53). The wireless

key comprises a programmable memory (54), a second central processing unit (55), and a transmitter (52), the wireless key being physically separate from the secure receptacle and typically stored in locations inaccessible to unauthorized users of the secure receptacle. The wireless key further possesses a plurality of buttons (56), the plurality of buttons being used to enter an access code. The second central processing unit (55) of the wireless key proceeds to determine whether the access code entered is consistent with the access code stored in the programmable memory (54). Upon the central processing unit (55) determining that the access code entered is acceptable, the transmitter (52) of the wireless key transmits a signal to the antenna (50) when the user pushes the "OPEN" button. The first central processing unit (51) receives a signal from the antenna (50) and subsequently disengages the locking mechanism (57) to allow access to the interior of the secure receptacle.

#### Example 5

Another embodiment of the invention, as shown in FIG. 7, involves a receiving unit comprising an antenna (60), a programmable memory (61), and a central processing unit (62). The receiving unit is cooperatively positioned within a secure receptacle, with the central processing unit (61) communicatively connected to the antenna (60) and the programmable memory (62), and the antenna communicatively connected to a transmitter (63) of a wireless key via a wireless link (64). The wireless key comprises a transmitter (63) that transmits a plurality of unlocking signals in sequential order, with one unlocking signal being sent upon the pushing of one of the plurality of buttons (65) of the wireless key. The plurality of unlocking signals are received by the antenna (60) and processed by the central processing unit (61). If the sequence of unlocking signals transmitted by the wireless key is consistent with the access code stored in the programmable memory (62), the central processing unit (61) disengages the locking mechanism (66) of the secure receptacle, thereby allowing the user of the wireless key access to the interior of the receptacle.

#### Example 6

The invention is further directed towards a process for the delivery of a retail good, the steps comprising the programming at least one programmable access code into a programmable memory (shown as 70 in FIG. 8); the ordering through a first

telecommunications device by a user at least one retail good from a supplier (shown as 71 in FIG. 8); delivering at least one retail good by the supplier to a secure receptacle (shown as 72 in FIG. 8); the user entering a user access code into a wireless key (shown as 73 in FIG. 8), the wireless key being physically separate from the secure receptacle to  
5 avoid accessibility by unauthorized parties; processing the user access code entered into the wireless key (shown as 74 in FIG. 8); and disengaging a locking mechanism of the secure receptacle (shown as 75 in FIG. 8), thereby allowing the user to gain access to at least one retail good previously ordered and delivered.

#### Example 7

10 In a further embodiment of the invention as shown in FIG. 9, a process for the delivery of a retail good employs two access codes, one that is entered through the use of a wireless key, the second which is entered through a keypad that is physically integrated with the secure receptacle. The process associated with the use of two access codes comprises the steps of programming at least one primary programmable access code  
15 into a first programmable memory that is integrated with the wireless key (shown as 80 in FIG. 9); programming at least one secondary programmable access code into a second programmable memory (shown as 81 in FIG. 9), the second programmable memory being integrated a keypad mounted to the secure receptacle; a user of a secure receptacle ordering at least one retail good from a supplier and the delivery of the order  
20 to the secure receptacle by the supplier's delivery carrier, entering a primary user access code by the user into a wireless key (shown as 82 in FIG. 9), the wireless key being physically separate from the secure receptacle; entering a secondary user access code by the user into a keypad (shown as 83 in FIG. 9), the keypad being physically integrated to the secure receptacle; processing the primary user access code entered into the  
25 wireless key and the secondary user access code entered into the keypad (shown as 84 in FIG. 9); and disengaging the locking mechanism of the secure receptacle (shown as 85 in FIG. 9), thereby allowing the user to gain access to at least one retail good previously ordered and delivered.

#### Example 8

30 A further embodiment of the invention is directed towards a process to inform the consumer of how much space remains in his or her secure receptacle as more and more



items are ordered. Of course, the secure or efficient delivery of items may be frustrated if too many items are ordered and they must either be left unattended by the secure receptacle or delivered at another time. Accordingly, when the consumer is placing an order through the Internet, an icon is presented which informs the consumer about the amount of space remains in his or her receptacle for the purchase of further retail goods. The process encompasses the ordering a plurality of retail goods through the Internet (shown as 90 in FIG. 10); providing a secure receptacle to the user with a predefined volume to which the plurality of retail goods will be delivered by a delivery carrier; calculating the percent volume a retail good ordered by the consumer will occupy in the secure receptacle when the retail good is placed in the secure receptacle by a delivery carrier (shown as 91 in FIG. 10); summing the percent volume for each retail good ordered by the user to obtain a total percent volume occupied by the plurality of retail goods; indicating the total percent volume to the user through the Internet while the user is ordering the plurality of retail goods (shown as 92 in FIG. 10); and resetting the total percent volume to zero after the user removes the plurality of retail goods from the secure receptacle.

#### Example 9

In another embodiment of the invention, a first unlocking signal is sent by the wireless key via a cellular wireless network, in which the wireless key can be a cellular telephone or a RIM 902M Radio Modem that is manufactured by Research in Motion, Ltd. The buttons of such devices are used to input the access code known by a party having authorization to gain entry to the secure receptacle. Upon the input of the access code, the unlocking signal is transmitted via the cellular network to a central server. The central server processes the unlocking signal and sends a second unlocking signal to a modem that is found within the interior of the secure receptacle. The modem is coupled to a central processing unit, the central processing unit in turn being coupled to a programmable memory and a locking mechanism for the receptacle. Upon the modem receiving the second unlocking signal, the central processing unit coupled to the programmable memory determines whether the second unlocking signal is consistent with the access code stored within the programmable memory. If the second

unlocking signal is consistent, the central processing unit disengages the locking mechanism of the receptacle, thereby allowing entry.

The wireless key in any of the embodiments of the invention possesses several means to discriminate against those who attempt to transmit an unlocking signal from the wireless key but are not authorized to do so. First, the wireless key is not attached to the secure receptacle and when not in use is stored in a location typically inaccessible to unauthorized users. Thus, the wireless key operates as a remote control and is only likely to be in the possession of only those parties who are authorized to gain access to the secure receptacle. Only under certain scenarios will an unauthorized party have possession of the wireless key, such as when the wireless key is lost or stolen.

Other embodiments of the wireless key also enhance security. In one embodiment of the invention, the wireless key possesses a plurality of buttons or means for entering data on the face of the wireless key. To gain access to the secure receptacle, an access code must be entered by depressing or pushing a combination of these buttons in a specific and predetermined sequence. The buttons may be labeled with alphanumeric indicia or color indicia.

For example, the wireless key may have ten buttons labeled with the numbers 0-9, respectively, with an access code consisting of a three-digit number which must be entered using the wireless key. Another example involves a wireless key possessing six buttons that uses color to distinguish between the different buttons, with the access code consisting of a color sequence, such as red-blue-red-yellow. Those skilled in the art will recognize that the use of alphanumeric and color indicia to create access restrictions will have many variations, both in the number of buttons possessed by the wireless key and the number of alphanumeric or color indicia that are used to create an access code.

The wireless key may employ other means which are capable of distinguishing an authorized user of the wireless key from an unauthorized user. As discussed above, knowledge of an access code distinguishes between authorized and non-authorized users. However, other criteria involving knowledge may be used, such as birth dates, maiden names, and social security numbers. In other embodiments, authorized and unauthorized users can also be distinguished by the use of physical characteristics of the

authorized user. Examples of this method include voice printing and finger printing, wherein the wireless key possesses a means to distinguish the voice or finger print of an authorized user from an unauthorized user. A Breathalyzer can also be integrated into any of the above embodiments of the wireless key to ensure the sobriety of the authorized user.

In the embodiments in which knowledge-based criteria are used to distinguish authorized users from non-authorized users, an additional level of security is gained by the ability to alter such knowledge-based access codes. This allows an authorized party to change an access code to prevent others who once had knowledge of the previous access code from now gaining access to the receptacle.

In another embodiment of the invention, a wireless key is used in conjunction with a keypad that is physically integrated with the secure receptacle. An authorized user desiring access to the secure receptacle will enter a primary access code into the wireless key and a secondary access code into the keypad. The primary access code will be processed in accordance with the means previously disclosed, while the secondary access code will be processed with a central processing unit communicatively coupled to the keypad. Upon the processing of both the primary and secondary access codes, the locking mechanism of the secure receptacle is disengaged.

A knowledge-based access code may be altered by many means, and the method employed is dependent upon the embodiment of the invention. For example, if the wireless key directly transmits the unlocking signal directly to the wireless link that is contained within the interior of the receptacle as previously described, both the programmable memory of the wireless key and the programmable memory of the wireless link must be edited. The programmable memory of the wireless key can be programmed using a programming device, such as internally through the use of buttons contained on the wireless key. For example, depressing the "OPEN" and "0" button simultaneously will allow a new access code to be entered and stored within the programmable memory of the wireless key. The programmable memory of the wireless link can be similarly programmed using a keypad attached to the receptacle and coupled to the central processing unit.

The programming of at least one programmable access code into a

programmable memory can be accomplished by several means. The user desiring to use a certain access code can access a web site to designate the desired access code. When the delivery carrier is delivering a retail good to the secure receptacle, the delivery carrier's wireless key downloads the desired programmable access code from the web site. The carrier's wireless key then transmits the desired access code via a low frequency signal to a wireless link physically integrated with the secure receptacle. The desired access code is subsequently uploaded to the programmable memory.

In a further embodiment of the invention, the programming of at least one programmable access code into a programmable memory can be accomplished through the use of the Internet. The user enters the desired access code through the use of a web site. The desired access code is downloaded to a modem from the web site through the Internet. The modem is physically integrated with the secure receptacle and communicatively coupled to the programmable memory. After downloading the desired access code from the web site, it is uploaded to the programmable memory.

The programming of at least one programmable access code into a programmable memory can further be accomplished through the use of a keypad physically integrated with the secure receptacle and communicatively coupled to the programmable memory. The user enters the code using the keys of the keypad and the desired code is uploaded to the programmable memory.

What is claimed is:

1. A system for the secure delivery of a retail good comprising:

a wireless key comprising a first cellular telephone that transmits a first unlocking  
5 signal to a geographically distant central server, the wireless key physically  
separate from a secure receptacle,

a receiving unit, the receiving unit comprising a central processing unit  
communicatively connected to a programmable memory, the receiving unit  
cooperatively positioned with the secure receptacle and communicatively  
10 connected to the geographically distant central server, said receiving unit  
receiving a second unlocking signal from the geographically distant central  
server,

the secure receptacle comprising a cover and a body, the body defining an interior  
within the secure receptacle, the body configured to possess an opening from  
15 which a retail good can be placed or removed from the interior of the secure  
receptacle, and the body further dimensioned to receive a plurality of retail  
goods,

the secure receptacle further comprising a locking mechanism communicatively  
coupled to the central processing unit and cooperatively positioned to securely  
20 engage the cover against the body and over the opening, thereby preventing  
access to the interior of the secure receptacle when desirable,

at least one access code stored in the programmable memory, of which one of the  
secure access codes comprises a current secure access code, and

the wireless key further comprising a face and a plurality of buttons, the plurality of  
25 buttons located on the face, a combination of the buttons comprising the current  
secure access code, a successful entry of the current secure access code using  
the buttons resulting in the processing of the second unlocking signal by the  
central processing unit and the subsequent release of the locking mechanism to  
allow the cover to be displaced from over the opening of the secure receptacle.

30 2. The system of claim 1, wherein the plurality of buttons comprise buttons

marked with alphanumeric indicia.

3. The system of claim 1, wherein the programmable memory stores more than one code, and a code system contained in the programmable memory and executed by  
5 the central processing unit selects the current access code.

4. The system of claim 1, wherein the geographically distant central server is communicatively connected to the receiving unit through the Internet.

10 5. The system of claim 1, wherein the receiving unit further comprises a pager, the pager communicatively connected to the central processing unit.

6. The system of claim 1, wherein the receiving unit further comprises a second cellular telephone, the second cellular telephone communicatively connected to the  
15 central processing unit.

7. The system of claim 1, wherein the receiving unit further comprises a modem, the modem communicatively connected to the central processing unit.

20 8. The system of claim 1, wherein the receiving unit further comprises a computer within a residence of a user, the computer communicatively connected to the central processing unit.

9. The system of claim 1, wherein the input device comprises a keypad  
25 cooperatively positioned to the secure receptacle and communicatively connected to the central processing unit, the keypad used to alter any of the secure access codes stored in the programmable memory.

10. The system of claim 9, wherein the input device comprises a keypad  
30 cooperatively positioned with the secure receptacle.

11. The system of claim 9, wherein the input device comprises the wireless key.

12. The system of claim 9, wherein the input device comprises a computer within a residence of a user.

5

13. A system for the secure delivery of a retail good comprising:

a wireless key comprising a two-way pager that transmits a first unlocking signal to a geographically distant central server, the wireless key physically separate from a secure receptacle,

10 a receiving unit, the receiving unit comprising a central processing unit communicatively connected to a programmable memory, the receiving unit cooperatively positioned with the secure receptacle and communicatively connected to the geographically distant central server, said receiving unit receiving a second unlocking signal from the geographically distant central server,

15

the secure receptacle comprising a cover and a body, the body defining an interior within the secure receptacle, the body configured to possess an opening from which a retail good can be placed or removed from the interior of the secure receptacle, and the body further dimensioned to receive a plurality of retail goods,

20

the secure receptacle further comprising a locking mechanism communicatively coupled to the central processing unit and cooperatively positioned to securely engage the cover against the body and over the opening, thereby preventing access to the interior of the secure receptacle when desirable,

25

at least one access code stored in the programmable memory, of which one of the secure access codes comprises a current secure access code, and

the wireless key further comprising a face and a plurality of buttons, the plurality of buttons located on the face, a combination of the buttons comprising the current secure access code, a successful entry of the current secure access code using the buttons resulting in the processing of the second unlocking signal by the central processing unit and the subsequent release of the locking mechanism to

30

allow the cover to be displaced from over the opening of the secure receptacle.

14. The system of claim 13, wherein the plurality of buttons comprise buttons marked with alphanumeric indicia.

5

15. The system of claim 13, wherein the programmable memory stores more than one code, and a code system contained in the programmable memory and executed by the central processing unit selects the current access code.

10 16. The system of claim 13, wherein the geographically distant central server is communicatively connected to the receiving unit through the Internet.

17. The system of claim 13, wherein the receiving unit further comprises a second pager, the second pager communicatively connected to the central processing unit.

15

18. The system of claim 13, wherein the receiving unit further comprises a cellular telephone, the cellular telephone communicatively connected to the central processing unit.

20 19. The system of claim 13, wherein the receiving unit further comprises a modem, the modem communicatively connected to the central processing unit.

20. The system of claim 13, wherein the receiving unit further comprises a computer within a residence of a user, the computer communicatively connected to the  
25 central processing unit.

30

21. The system of claim 13, wherein an input device is communicatively connected to the central processing unit, the input device used to alter any of the secure access codes stored in the programmable memory.

22. The system of claim 21, wherein the input device comprises a keypad



cooperatively positioned with the secure receptacle.

23. The system of claim 21, wherein the input device comprises the wireless key.

5 24. The system of claim 21, wherein the input device comprises a computer within a residence of a user.

25. A system for the secure delivery of a retail good comprising:

10 a wireless key comprising a computer within a residence of a user that transmits a first unlocking signal to a geographically distant central server, the wireless key physically separate from a secure receptacle,

a receiving unit, the receiving unit comprising a central processing unit

15 communicatively connected to a programmable memory, the receiving unit cooperatively positioned with the secure receptacle and communicatively connected to the geographically distant central server, said receiving unit receiving a second unlocking signal from the geographically distant central server,

20 the secure receptacle comprising a cover and a body, the body defining an interior within the secure receptacle, the body configured to possess an opening from which a retail good can be placed or removed from the interior of the secure receptacle, and the body further dimensioned to receive a plurality of retail goods,

25 the secure receptacle further comprising a locking mechanism communicatively coupled to the central processing unit and cooperatively positioned to securely engage the cover against the body and over the opening, thereby preventing access to the interior of the secure receptacle when desirable,

at least one access code stored in the programmable memory, of which one of the secure access codes comprises a current secure access code, and

30 the wireless key further comprising a face and a plurality of buttons, the plurality of buttons located on the face, a combination of the buttons comprising the current secure access code, a successful entry of the current secure access code using

the buttons resulting in the processing of the second unlocking signal by the central processing unit and the subsequent release of the locking mechanism to allow the cover to be displaced from over the opening of the secure receptacle.

- 5      26.    The system of claim 25, wherein the plurality of buttons comprise buttons marked with alphanumeric indicia.
27.    The system of claim 25, wherein the programmable memory stores more than one code, and a code system contained in the programmable memory and executed by  
10    the central processing unit selects the current access code.
28.    The system of claim 25, wherein the geographically distant central server is communicatively connected to the receiving unit through the Internet.
- 15    29.    The system of claim 25, wherein the receiving unit further comprises a pager, the pager communicatively connected to the central processing unit.
30.    The system of claim 25, wherein the receiving unit further comprises a cellular telephone, the cellular telephone communicatively connected to the central processing  
20    unit.
31.    The system of claim 25, wherein the receiving unit further comprises a modem, the modem communicatively connected to the central processing unit.
- 25    32.    The system of claim 25, wherein the receiving unit further comprises the computer within a residence of a user, the computer communicatively connected to the central processing unit.
33.    The system of claim 25, wherein an input device is communicatively connected  
30    to the central processing unit, the input device used to alter any of the secure access codes stored in the programmable memory.

34. The system of claim 33, wherein the input device comprises a keypad cooperatively positioned with the secure receptacle.

35. The system of claim 33, wherein the input device comprises the wireless key.

5

36. The system of claim 33, wherein the input device comprises the computer within a residence of a user.

37. A system for the secure delivery of a retail good comprising:

10 a receiving unit comprising an antenna and a first central processing unit, the receiving unit cooperatively positioned with a secure receptacle, the first central processing unit communicatively connected to the antenna, and the antenna communicatively connected to a wireless key via a wireless link,  
the wireless key comprising a programmable memory, a second central processing unit,  
15 and a transmitter that transmits an unlocking signal that is received by the antenna, the wireless key physically separate from the secure receptacle, the secure receptacle comprising a cover and a body, the body defining an interior within the secure receptacle, the body configured to possess an opening from which a retail good can be placed or removed from the interior of the secure receptacle, and the body further dimensioned to receive a plurality of retail  
20 goods,  
the secure receptacle further comprising a locking mechanism communicatively coupled to the first central processing unit and cooperatively positioned to securely engage the cover against the body and over the opening, thereby  
25 preventing access to the interior of the secure receptacle when desirable, at least one secure access code stored in the programmable memory of which one of the secure access codes comprises a current secure access code, and  
the wireless key further comprising a face and a plurality of buttons, the plurality of  
30 buttons located on the face, a combination of the buttons comprising the current secure access code, a successful entry of the current secure access code using the buttons processed by the second central processing unit and resulting in the

transmission of the unlocking signal via the wireless link to the receiving unit and the release of the locking mechanism to allow the cover to be displaced from over the opening of the secure receptacle.

5      38.      The system of claim 37, wherein the plurality of buttons comprise buttons marked with alphanumeric indicia.

39.      The system of claim 37, wherein the plurality of buttons comprise buttons marked with color indicia.

10

40.      The system of claim 37, wherein the programmable memory stores more than one code and a code system contained in the programmable memory and executed by the first central processing unit selects the current access code.

15      41.      The system of claim 37, wherein a programming device is communicatively coupled to the programmable memory to upload at least one access code.

42.      The system of claim 37, wherein the plurality of buttons on the face of the wireless key are communicatively coupled to the programmable memory to upload at  
20      least one access code.

43.      A system for the secure delivery of a retail good comprising:  
a receiving unit comprising an antenna, a programmable memory and a central  
processing unit, the receiving unit cooperatively positioned with a secure  
25      receptacle, the central processing unit communicatively connected to the  
antenna and the programmable memory, and the antenna communicatively  
connected to a wireless key via a wireless link,  
the wireless key comprising a transmitter that transmits a plurality of unlocking signals  
in sequential order, the plurality of unlocking signals received by the antenna,  
30      the wireless key physically separate from the secure receptacle,  
the secure receptacle comprising a cover and a body, the body defining an interior

within the secure receptacle, the body configured to possess an opening from which a retail good can be placed or removed from the interior of the secure receptacle, and the body further dimensioned to receive a plurality of retail goods,

- 5 the secure receptacle further comprising a locking mechanism communicatively coupled to the central processing unit and cooperatively positioned to securely engage the cover against the body and over the opening, thereby preventing access to the interior of the secure receptacle when desirable,
- 10 at least one secure access code stored in the programmable memory of which one of the secure access codes comprises a current secure access code, and the wireless key further comprising a face and a plurality of buttons, the plurality of buttons located on the face, a combination of the buttons comprising the current secure access code, a successful entry of the current secure access code using the buttons resulting in the transmission of the plurality of unlocking signals via
- 15 the wireless link to the antenna, the processing of the plurality of unlocking signals by the central processing unit, and the release of the locking mechanism to allow the cover to be displaced from over the opening of the secure receptacle.

20 44. The system of claim 43, wherein the plurality of buttons comprise buttons marked with alphanumeric indicia.

45. The system of claim 43, wherein the plurality of buttons comprise buttons marked with color indicia.

25 46. The system of claim 43, wherein the programmable memory stores more than one code and a code system contained in the programmable memory and executed by the central processing unit selects the current access code.

30 47. The system of claim 43, wherein an input device is communicatively connected to the central processing unit, the input device used to alter any of the secure access

codes stored in the programmable memory.

48. The system of claim 47, wherein the input device comprises a keypad cooperatively positioned with the secure receptacle.

5

49. The system of claim 47, wherein the input device comprises the wireless key.

50. A process for the delivery of a retail good, comprising the steps of:  
programming at least one programmable access code into a programmable  
memory,

10

ordering through a first telecommunications device by a user at least one retail good  
from a supplier,

delivering at least one retail good by the supplier to a secure receptacle,  
entering a user access code by the user into a wireless key, the wireless key being

15

physically separate from the secure receptacle,  
processing the user access code entered into the wireless key, and  
disengaging a locking mechanism of the secure receptacle, thereby allowing the user to  
gain access to at least one retail good previously ordered and delivered.

20

51. The process of claim 50, wherein the access code comprises knowledge-based  
information that distinguishes the user who ordered at least one retail good from an  
unauthorized user attempting to gain access to the secure receptacle.

25

52. The process of claim 51, wherein the access code comprises a combination of  
alphanumeric characters.

53. The process of claim 51, wherein the access code comprises a combination of  
colors.

30

54. The process of claim 50, wherein the access code comprises physical  
characteristics of the user.

55. The process of claim 54, wherein the physical characteristic of the user comprises a finger print.

5 56. The process of claim 54, wherein the physical characteristic of the user comprises a voice print.

57. The process of claim 50, wherein the programming the programmable access code into the programmable memory comprises the steps of:  
10 downloading from a web site to a supplier's wireless key the programmable access code, the programmable access code previously designated by the user, transmitting the programmable access code by a low frequency signal to a receiving unit physically integrated with the secure receptacle, and  
15 uploading the programmable access code into the programmable memory from the receiving unit.

58. The process of claim 50, wherein the programming the programmable access code into the programmable memory comprises the steps of:  
accessing a modem through the Internet, the modem being physically integrated with  
20 the secure receptacle and communicatively coupled to the programmable memory,  
downloading from the Internet the programmable access code designated by the user, and  
uploading the programmable access code into the programmable memory.

25 59. The process of claim 50, wherein the programming the programmable access code into the programmable memory comprises the steps of:  
entering the programmable access code using a keypad physically integrated with the secure receptacle and communicatively coupled to the programmable memory,  
30 and  
uploading the programmable access code to the programmable memory.

60. The process of claim 50, wherein processing the access code further comprises the steps of:

5 comparing the user access code entered by the user with the programmable access code programmed into the programmable memory, the programmable memory physically integrated with the wireless key, pushing a button on the wireless key by the user to transmit a low-frequency radio wave signal, and transmitting the low-frequency radio wave signal from the wireless key to a receiving unit physically integrated with the secure receptacle, a receiving unit  
10 communicatively connected to the locking mechanism of the secure receptacle, the receiving unit comprising an antenna and a central processing unit.

61. The process of claim 60, wherein processing the access code further comprises the step of testing the sobriety of the user through a means for detecting a blood alcohol  
15 content.

62. The process of claim 50, wherein processing the access code further comprises the steps of:

20 transmitting a first unlocking signal from a second telecommunications device to a geographically distant central server, transmitting a second unlocking signal from the geographically distant central server to a receiving unit, the receiving unit physically integrated with the secure receptacle and communicatively coupled to a central processing unit, the central  
25 processing unit further communicatively coupled to the locking mechanism, and comparing the user access code entered by the user with the programmable access code programmed into the programmable memory, the programmable memory physically integrated with secure receptacle and communicatively coupled to the central processing unit.

30 63. The process of claim 62, wherein the second telecommunications device



comprises a pager.

64. The process of claim 62, wherein the second telecommunications device comprises a first cellular telephone.

5

65. The process of claim 62, wherein the receiving unit comprises a modem.

66. The process of claim 62, wherein the receiving unit comprises a second cellular telephone.

10

67. The process of claim 62, wherein the receiving unit comprises a two-way pager.

68. The process of claim 62, wherein the receiving unit comprises a home computer within a residence of a user.

15

69. A process for the delivery of a retail good, comprising the steps:  
programming at least one primary programmable access code into a first programmable memory,

20

programming at least one secondary programmable access code into a second programmable memory,

ordering through a first telecommunications device at least one retail good from a supplier by a user,

delivering at least one retail good by the supplier to a secure receptacle,

entering a primary user access code by the user into a wireless key, the wireless key

25

being physically separate from the secure receptacle,

entering a secondary user access code by the user into a keypad, the keypad being physically integrated to the secure receptacle,

processing the primary user access code entered into the wireless key,

processing the secondary user access code entered into the keypad, and

30

disengaging a locking mechanism of the secure receptacle, thereby allowing the user to gain access to at least one retail good previously ordered and delivered.

70. The process of claim 69, wherein the primary and secondary access codes comprise knowledge-based information that distinguishes the user who ordered at least one retail good from an unauthorized user attempting to gain access to the secure receptacle.

5

71. The process of claim 69, wherein the primary and secondary access codes comprise a combination of alphanumeric characters.

10

72. The process of claim 69, wherein the primary access code comprises a combination of colors.

73. The process of claim 69, wherein the primary access code comprises physical characteristics of the user.

15

74. The process of claim 73, wherein the physical characteristic of the user comprises a finger print.

75. The process of claim 73, wherein the physical characteristic of the user comprises a voice print.

20

76. A process for ordering a plurality of retail goods, comprising the steps of:  
ordering the plurality of retail goods through the Internet by a user,  
providing a secure receptacle to the user with a predefined volume to which the  
plurality of retail goods will be delivered by a delivery carrier,  
25 calculating the percent volume a retail good ordered by the consumer will occupy in the  
secure receptacle when the retail good is placed in the secure receptacle by a  
delivery carrier,  
summing the percent volume for each retail good ordered by the user to obtain a total  
percent volume occupied by the plurality of retail goods,  
30 indicating the total percent volume to the user through the Internet while the user is  
ordering the plurality of retail goods, and

resetting the total percent volume to zero after the user removes the plurality of retail goods from the secure receptacle.

5        77.     The process of claim 76, wherein the total percent volume consists of summing the percent volume for each retail good ordered by the user in a plurality of orders by the consumer and before.

10       78.     The process of claim 77, wherein the plurality of orders comprise orders between different suppliers.

15       79.     The process of claim 77, wherein the plurality of orders comprise orders between different times at which the user places an order.

1/5

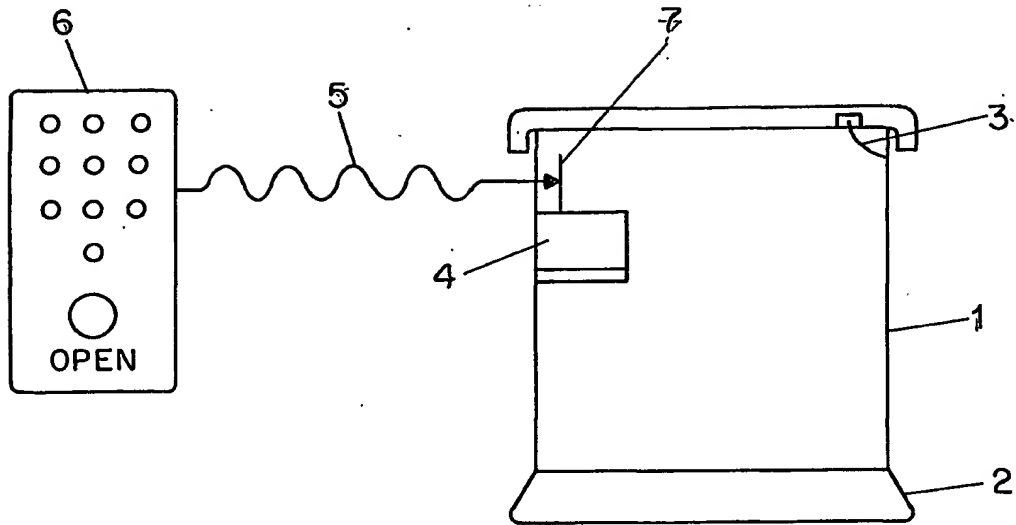


FIG. 1

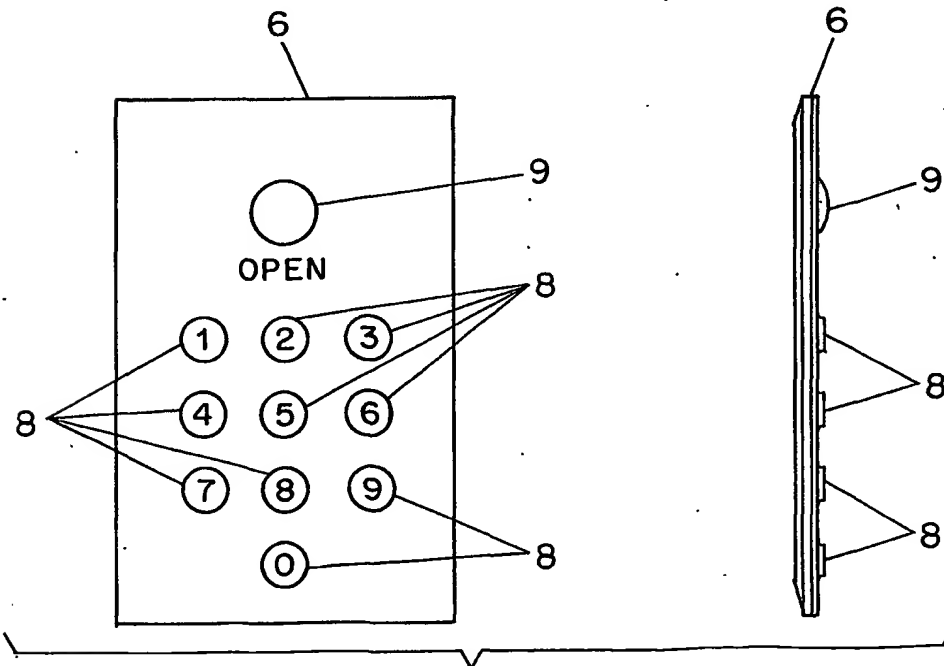


FIG. 2

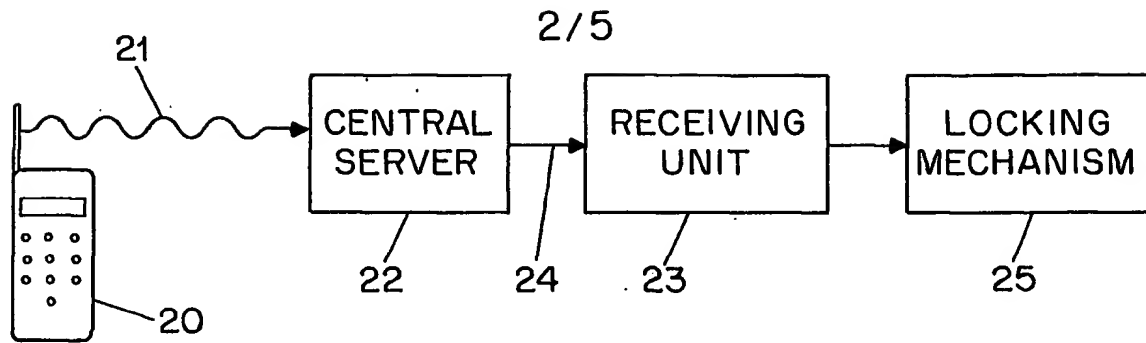


FIG. 3

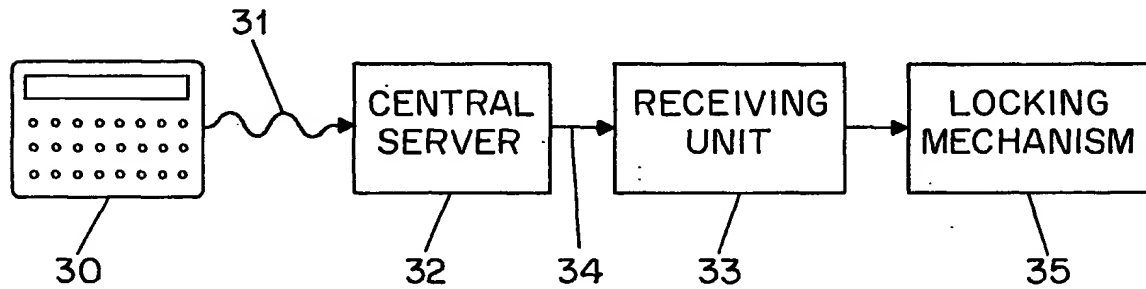


FIG. 4

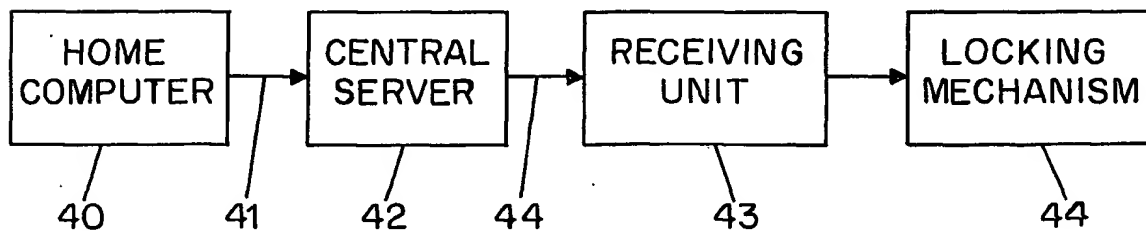


FIG. 5

3/5

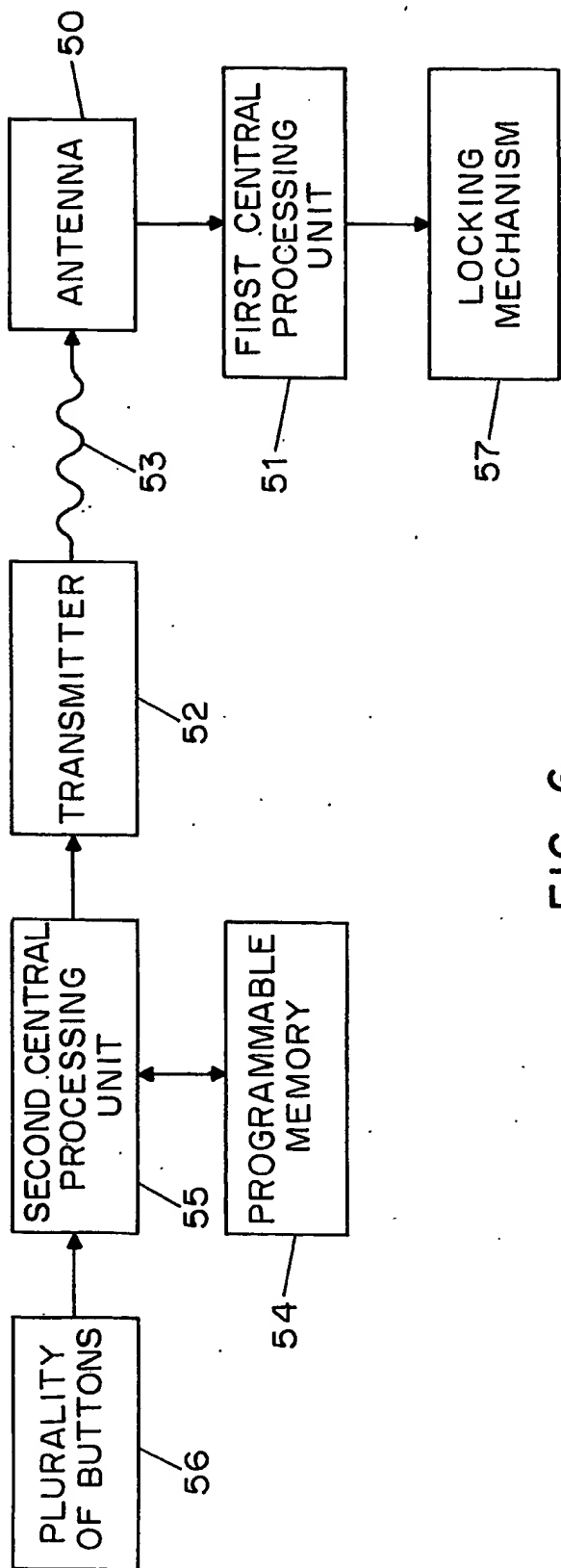


FIG. 6

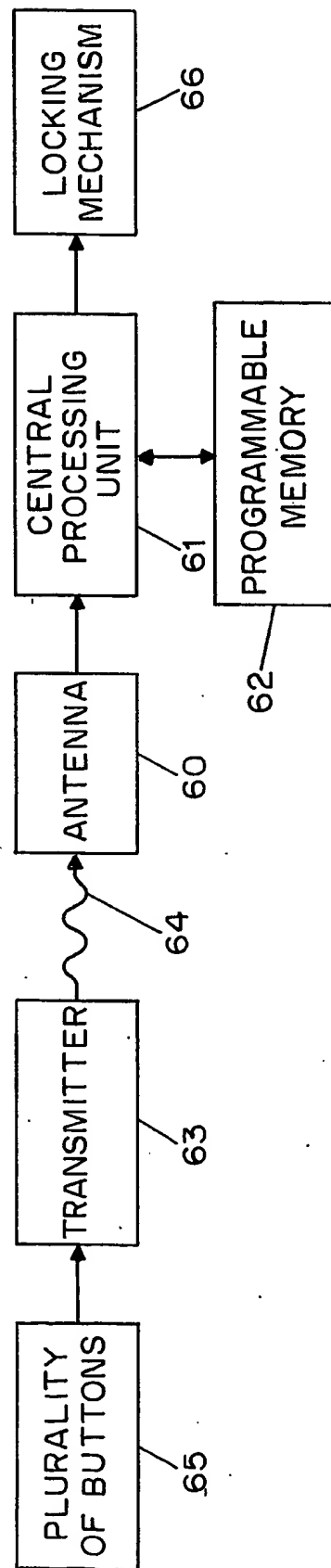


FIG. 7

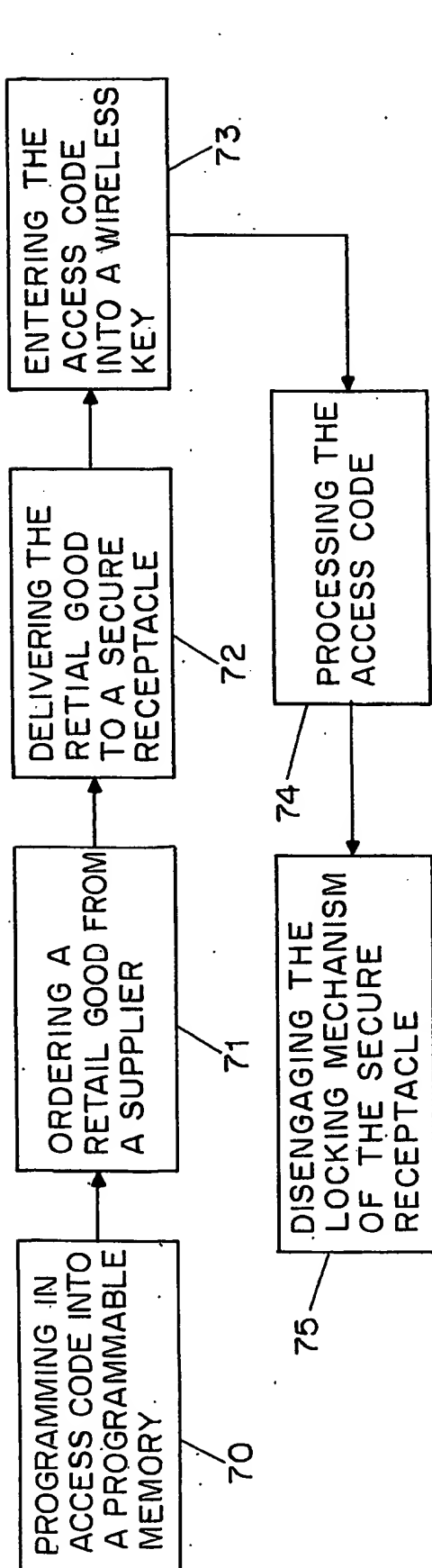


FIG. 8

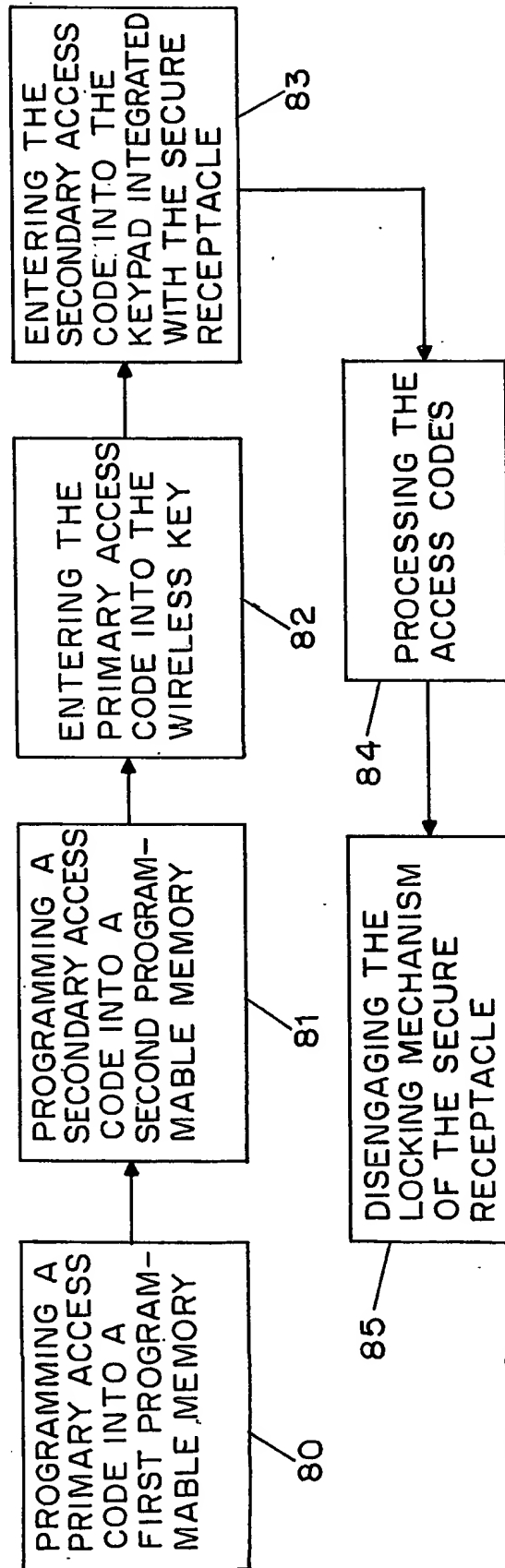


FIG. 9

5/5

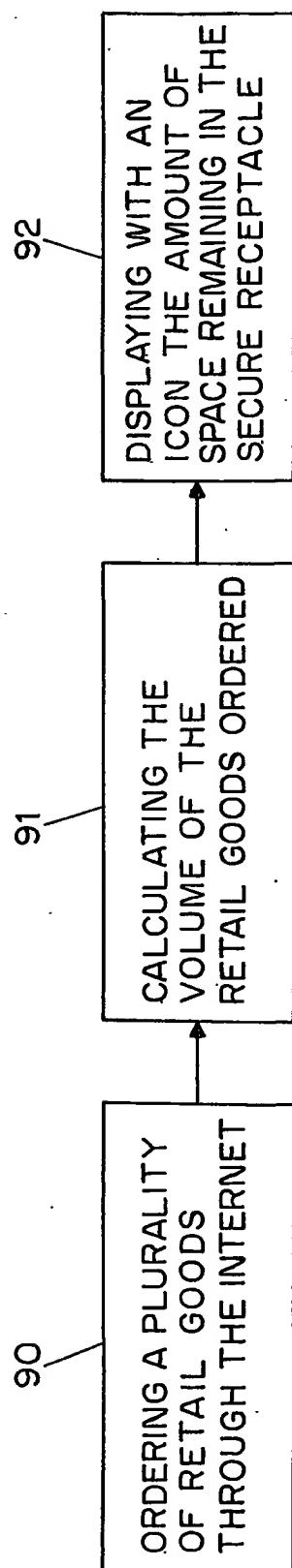


FIG. 10



## INTERNATIONAL SEARCH REPORT

International application No.

PCT/US01/26840

## A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) :G06F 7/04

US CL :340/825.31, 34/10.31; 342/457

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 340/825.31, 34/10.31; 342/457; 340/5.1, 5.2, 5.6, 5.71, 5.73, 5.74, 825.71, 825.72

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EAST

search terms: (wireless key or cellular phone) and (security or authorized or access code) and (locks or unlocks) and deliver\$

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category <sup>o</sup>	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y,P	US 6,323,782 A (STEPHENS ET AL) 27 November 2001, entire document.	1-79
Y	US 5,942,985 A (CHIN) 24 AUGUST 1999, Title, Abstract, Figures 1 and 2, columns 2-3, col. 6, lines 1-28.	1-75
Y	US 5,774,053 A (PORTER) 30 JUNE 1998, title, abstract, Figures 1, 2, 3, 4, and 5, Col. 1, lines 20-26, col. 4, lines 10-21, col. 5, lines 15-28, columns 7-8.	1-79
Y	US 5,991,749 A (MORRILL, JR.) 23, NOVEMBER 1999, title, col. 3, lines 45-65.	1-49
Y	US 5,966,663 A (GLEASON) 12 OCTOBER 1999, Abstract, Figure 1.	4, 16 and 28



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E" earlier document published on or after the international filing date	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L" document which may throw doubt on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"A" document member of the same patent family
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search 01 DECEMBER 2001	Date of mailing of the international search report 06 FEB 2002
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer LY V. HUA Telephone No. (703) 305-9684

## INTERNATIONAL SEARCH REPORT

International application No.  
PCT/US01/26840

## C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category <sup>o</sup>	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,491,807 A (FREEMAN ET AL) 13 FEBRUARY 1996, Figures 4 and 5, col. 4, lines 14-27.	76-79
Y	US 4,795,424 A (BURNER) 03 JANUARY 1989, col. 8, line 65 to col. 9, line 9.	76-79
Y	US 5,599,099 A (MANDEL ET AL) 04 FEBRUARY 1997, col. 20, lines 27-40.	76-79
Y	US 5,802,859 A (ZUGIBE) 08 SEPTEMBER 1998, col. 9, lines 34-55.	76-79